DEPARTMENT OF DEFENSE • DEFENSE SECURITY SERVICE, INDUSTRIAL SECURITY PROGRAM OFFICE

INDUSTRIAL SECURITY LETTER

Industrial Security letters will be issued periodically to inform Industry, User Agencies and DoD Activities of developments relating to industrial security. The contents of these letters are for information and clarification of existing policy and requirements. Local reproduction of these letters in their original form for the internal use of addressees is authorized. Suggestions and articles for inclusion in the Letter will be appreciated. Articles and ideas contributed will become the property of DSS. Contractor requests for copies of the Letter and inquiries concerning specific information should be addressed to their cognizant security office, for referral to the Industrial Security Program Office, Headquarters, DSS, as appropriate.

ISL 03L-1 **April 16, 2003**

1. 2002 Cogswell Award Recipients.

Mr. William A. Curtis, Acting Director, DSS, announced the 2002 DSS James S. Cogswell Outstanding Industrial Security Achievement Awards on September 12, 2002, during the American Society for Industrial Security's annual seminar in Philadelphia, PA. Twelve facilities were selected for the annual award that honors organizations that establish and continue to maintain an outstanding industrial security program. Congratulations to the following facilities:

Capital Area

Orbital Sciences Corporation
Dulles, VA

SRI International
Arlington, VA

Central Area

AVISYS, Inc.
Austin, TX

Ball Aerospace and Technologies Corporation, Dayton Office
Fairborn, OH

General Dynamics Land Systems, (Lima Army Tank Plant)
Lima, OH

Syracuse Research Corporation
San Antonio, TX

The Boeing Company
Tulsa, OK

Northeast Area

Goodrich Corporation, Optical & Space Systems
Lexington, MA

Southeast Area

Osborne Technologies, Inc.
Huntsville, AL

West Region

ATK Thiokol Propulsion
Corinne, UT

New Mexico Institute of Mining and Technology
Socorro, NM

Sverdrup Technology, Inc., Naval Systems Group
Camarillo, CA

2. Transfer of Personnel Security Investigations to the Office of Personnel Management.

The Department of Defense (DoD) and Office of Personnel Management (OPM) have entered into an agreement to transform the process for conducting personnel security investigations (PSI). As part of the FY 2004 budget sent to Congress, DoD will divest its PSI functions currently performed by DSS to OPM. Centralization of this function within the federal government will improve security, eliminate duplicative functions and maximize opportunities for cost savings and efficiencies. For industry, the transfer of the PSI function should be seamless. DISCO will remain a part of DSS and will continue to provide security clearance services for industry.

3. United Kingdom RESTRICTED Information.

On January 27, 2003, the United States Department of Defense (DoD) and the United Kingdom (UK) Ministry of Defence (MoD) signed a document known as the "Security Implementing Arrangement" that removed U.S. Government oversight responsibility for protection of information marked UK RESTRICTED provided to U.S. contractors. The UK Government implemented these changes effective April 1, 2003.

It is the responsibility of the contracting activity to incorporate requirements for the protection of UK RESTRICTED information into contracts. Attached to this ISL is a copy of the UK Government's "Restricted Conditions Requirements Clause." Questions relating to the safeguarding requirements under current contracts should be directed to your contracting activity.

Summary of Changes Related to U.S. Government Responsibilities

1. The requirements of the National Industrial Security Program Operating Manual (NISPOM) no longer apply to UK RESTRICTED information.

2. A contractor's responsibility for safeguarding UK RESTRICTED information is now a contractual obligation.

3. UK RESTRICTED information provided to U.S. industry will no longer be subject to oversight by DSS.

4. Neither a personnel nor facility security clearance is required for access to UK RESTRICTED information.

5. UK RESTRICTED information may be transmitted directly to U.S. industry by the UK MoD (and its contractors).

6. UK RESTRICTED documents may be single wrapped and transmitted by First Class Mail within the United States. Transmissions outside the United States must be doubled wrapped with the inner envelope marked "UK RESTRICTED." International transfers shall be by one of the means

authorized for U.S. classified information, by international airmail, or by express commercial courier services. Government-to-government transmission procedures are not required.

7. UK RESTRICTED information may be transmitted or accessed electronically via a public network like the Internet using government or commercial encryption devices approved by the MoD. Telephone conversations, video conferencing or facsimile transmissions within the United States may be conducted without encryption. International telephone conversations, video conferencing or facsimile transmissions containing UK RESTRICTED information may be conducted without encryption if an approved encryption system is not available.

8. Guidance regarding the use of communications and information systems for storing, processing and transmitting UK RESTRICTED information will be incorporated into the Restricted Conditions Requirements Clause in the contract. Contractors are authorized to self-certify and accredit information systems using guidance provided to them in the Restricted Conditions Requirements Clause.

9. Contracts placed with US contractors that involve the retention or production of UK RESTRICTED information will include a Restricted Conditions Requirements Clause identifying the security protective measures to be applied to safeguard the information. Unless prohibited by the contract, contractors may subcontract to contractors in the US or the UK without prior approval of the UK contracting authority. The Restricted Conditions Requirements Clause shall be included in any subcontract requiring access to UK RESTRICTED information. Subcontracts must not be awarded to any facility located outside the US or the UK without the written approval of the UK contracting authority.

10. When the US DoD provides UK RESTRICTED information to either US or UK industry, it will also provide safeguarding guidance.

11. An export license for UK RESTRICTED information should be processed as any other unclassified information would be processed. The information subject to export will not have to pass through government-to-government channels as described in NISPOM Section 10-4.

Specific Information Regarding Visits Involving Unclassified information or UK RESTRICTED information

Visits to UK MoD facilities and to contractor facilities in the United States or United Kingdom where the requirement for access is limited solely to Unclassified or UK RESTRICTED information do not require a government-sponsored visit authorization. Such visits can be arranged directly between the sending and receiving facilities. It is the responsibility of the US facility hosting a UK visitor to ensure that all export control and foreign disclosure requirements are satisfied prior to the disclosure of any information.

4. Inspecting Areas Above False Ceilings and Below Raised Floors in Closed Areas.

When a Closed Area has a false ceiling and/or raised floor, the areas above the false ceiling and below the raised floor are part of the Closed Area. These areas are often not visible, and may provide opportunities for surreptitious entry, modifications or tampering. Contractors must develop and implement procedures to ensure the continued structural integrity of Closed Areas. One of the following options may be selected.

a) Alarming the area above the false ceiling and/or below the raised floor.

b) Establishing certain ceiling tiles or installing clear tiles to facilitate viewing around the periphery of the area so that the integrity of the walls above the false ceiling and below the raised floor can be verified during normal operations.

c) Periodically inspecting the areas above the false ceilings or below the raised floors by removing ceiling or floor tiles. Minimum intervals for inspecting the areas will vary depending on the nature of classified material stored in the Closed Area and overall security of the cleared contractor facility. The following matrix is provided as a guideline for determining an appropriate minimum inspection frequency. While this matrix provides a guide, in certain instances an accelerated or decelerated inspection frequency may be appropriate based on conditions at specific cleared facilities. The required minimum inspection frequency must be approved by your Industrial Security Representative, and properly documented on the DSS Form 147, "Record of Controlled Areas."

Nature of Classified Information	Security-in-Depth	Minimum Inspection Frequency
Classified Information Systems with unprotected transmission lines above false ceiling or below false floor	No	Monthly
	Yes	Every Six Months
Open Storage of Classified Documents	No	Monthly
	Yes	Every Six Months
Classified Hardware[1]	No	Every Six Months
	Yes	Annually

5. Implementation of May 1, 2000 Chapter 8, Information System Security Requirements.

Question 2 of ISL 01L-1 established May 1, 2004 as the last date for upgrading all existing accredited Information Systems (IS) to the requirements of the May 1, 2000 NISPOM Chapter 8. With more than half of that time elapsed, there are many accredited IS that have not yet been upgraded to the new Chapter 8 requirements. This article is a reminder that after May 1, 2004, any IS not accredited against the May 1, 2000 Chapter 8 requirements will not be authorized to process classified information. Contact your DSS Industrial Security Representative or Information System Security Professional (ISSP) should you have any questions or require assistance.

6. PCL/FCL Requirements for Self-Employed Consultants.

Cleared contractors may process self-incorporated consultants for a PCL in accordance with NISPOM paragraph 2-213 provided the consultant and members of his/her immediate family are the sole owners of the consultant's company, and only the consultant requires access to classified information. In such cases,

[1] Storage of Confidential classified hardware and CSA approved open storage of Confidential documents does not require NISPOM supplemental controls/IDS. Approved open storage of Confidential material will require monthly checks of areas above false ceilings and below raised floors.

a facility security clearance (FCL) is not required, and payment can be made either in the name of the consultant or the consultant's firm. Should other employees of the consultant's company require access to classified information, it would constitute a classified subcontract, and as such, a DD Form 254 must be issued by the prime contractor, and the consultant's firm will require an FCL.

7. Submission of SF-312 to DISCO.

NISPOM Paragraph 3-105 requires that an individual issued an initial personnel security clearance (PCL) execute an SF-312, Classified Information Nondisclosure Agreement prior to being granted access to classified information, and that the facility submit the original SF-312 to DISCO for retention. Please note this requirement applies only to individuals granted an initial PCL. We are receiving numerous SF-312s for individuals that held a previous PCL that was converted or reinstated in accordance with NISPOM paragraphs 2-215 and 2-217. While use of the SF-312 in these instances to document a security briefing is permissible, contractors should not forward the completed SF-312 to DISCO.

8. Non-Possessing Division or Branch Office Facility Security Clearances.

Historically, multiple facility organizations (MFO's) have had the option to centralize and administer certain security functions such as personnel clearance administration, security education, and classified visit authorizations within home office locations, or other cleared locations (known as principal management facilities (PMF)). Companies exercising this option maximize security resources and, in requiring fewer facility security clearances, avoid the related additional (processing and maintenance) costs by government and industry. There are currently numerous non-possessing division or branch offices cleared under the NISP. These are facilities that already have viable security programs established at their home office locations. Those home office locations can, in most cases, effectively administer the limited security administrative functions for these branch office locations. Accordingly, DISCO will no longer process new facility security clearances (FCL) for division or branch offices that do not require possession of classified material for contract performance, unless there is a sufficient contractual or critical operational need.

Over the last several months, DSS has been contacting currently cleared non-possessing division or branch offices to review the organizational security structure and classified contract performance requirements. Based on that review, DSS has, when appropriate, proposed administrative termination of those facility clearances and transferred personnel security administrative functions to a cleared home office or PMF. DSS acknowledges that there may be rare exceptions when a non-possessing division or branch office may require a FCL. Examples would include a contractual requirement to establish a cleared branch office in proximity to the customer; or unusually high numbers of personnel security clearances (i.e. 200-300) needed at the division, and the additional personnel security administration responsibilities would place an undue burden on the Home Office or PMF. Facilities considering administrative termination of non-possessing division or branch offices may contact their assigned DSS Industrial Security Representative for further guidance.

9. Ensuring Clearance Requests are Reviewed for an Interim Determination.

As noted in ISL-00L-1, the Requester field in EPSQ for industrial personnel clearance requests must reflect DISCO to ensure the request is processed properly. Unfortunately, a significant number of improperly coded investigative requests are still being received. DISCO routinely reviews clearance requests to determine whether an interim personnel security clearance can be issued. In most cases, an interim determination is made within three days of receipt of the clearance request. Improperly coded

EPSQs are not immediately reviewed for Interim clearance determinations and often take significant time before they are identified as industrial clearance requests.

Instructions for completion of an EPSQ form can be found on the DSS web site (www.dss.mil), under the EPSQ section. These instructions include advice for industrial customers regarding information that should be included in the Facility Security Officer portion of the EPSQ to ensure the request is reviewed expeditiously by DISCO. The following summary is provided:

To ensure the clearance request is routed to DISCO

- "Return Results to" address must indicate DISCO
- DISCO is selected as the requestor
- Choose 4 (DISCO) from the drop down menu (NACLC & SPR)
- Select DISCO when certifying the user form (SSBI & SBPR)
- Organization Code is the facility CAGE Code
- Organization Code Type is the CAGE
- Requestor Name is the facility name and address

To avoid privacy issues:

- All reports for adjudication go to DISCO
- Return results to: DISCO, 2780 Airport Drive, Suite 400, Columbus, OH 43219-2268

Special Compartmented Information (SCI)

- Return results to: Appropriate Central Adjudicative Facility that will adjudicate the SCI.
- The requester is DISCO

If you still require assistance after reviewing these instructions, please contact the Customer Call Center, 1-800-542-0237, for technical assistance in setting up and using the EPSQ, or the Customer Service Branch, 1-888-282-7682, for other assistance.

10. Visit Authorization Letters for the Department of Energy (DoE).

The Department of Energy requires requests for access to Restricted Data in the possession of DoE or other Federal Agencies designated by DoE to be made utilizing DoE Form 277, "Request for Visit or Access Approval." For contractors, the need for access to Restricted Data will, in all cases, be certified by a Government Contracting Officer (GCO). Failure to utilize the DOE Form 277 has caused unnecessary delays for some cleared contractor employees in gaining access to information required for job performance.

11. Interim Access to JPAS – Based on NAC.

The paragraph "Clearance Requirements for Users" in article 3, ISL 02L-1 indicated the minimum requirement for access to the Joint Personnel Adjudication System (JPAS) is a SECRET PCL. Please note the requirement is actually a clearance "eligibility" investigation based on a NACLC. The NACLC became the required investigative basis for all SECRET and CONFIDENTIAL clearances in January 1999. Therefore, some individuals requiring access to JPAS will have a SECRET or CONFIDENTIAL clearance based on a National Agency Check. These individuals will be permitted interim access to JPAS provided they have submitted an EPSQ for a NACLC. In these cases, Item 6, "Reason for Request" in the "National Agency Check Security Information" section of EPSQ 2.2, should be annotated with the following statement: "NACLC required for JPAS access."

12. Reinstatements and Conversions of Personnel Security Clearances.

Article 5 of ISL 02L-1 discusses the waiver of the requirements of paragraphs 2-215 and 2-217 of the NISPOM. For the purpose of visit authorization letters, contractors have asked what date of clearance they should use when they use the waiver to reinstate or convert a clearance. Since the gaining facility is required to submit a DISCO Form 562 to DSS when the waiver is utilized, contractors should use the date of the DISCO Form 562 as the date of clearance until they receive the new Letter of Consent from DISCO.

13. Personnel Clearances, the Internet, and Job Seeking.

The NISPOM clearly prohibits the use of a Facility Clearance for advertising purposes (2-100c, NISPOM). However, individuals may address specific qualification requirements associated with a position by informing prospective employers that they have been granted a personnel clearance (PCL) at the requisite level identified for the position. Aside from addressing specific qualifications for a particular position at a cleared contractor or Government facility, it is a poor security practice to identify oneself in a public database as a cleared person and become flagged as a possible target for foreign interests. Examples of such flagging, or identifying oneself as a cleared person, include online Internet employment services that solicit clearance information as well as other personnel data, and make this publicly available by electronic means. It should be understood that the audience for the Internet is worldwide and includes a large number of domestic and foreign entities. Other examples of flagging are employment seminars or job fairs that invite only persons granted a clearance to attend and register. In general, these and similar situations may also provide opportunities for foreign targeting and collection efforts. Foreign entities may be interested in identifying individuals who access or can access classified information. It is recommended that persons granted a clearance should consider the prospective audience before identifying themselves as cleared.

14. Alarm System Description Form.

In accordance with NISPOM paragraph 5-901a, approval of an intrusion detection system (IDS) is based on the criteria of UL Standard 2050 or DCID 1/21 (Note: DCID 1/21 has subsequently been replaced by DCID 6/9). UL 2050 is the required Standard for contractors under DSS security cognizance, except in certain cases where an IDS has been approved by another cognizant security agency (CSA). UL 2050 requires a separate CRZH Certificate for each alarmed area. The Standard now also requires the Cognizant Security Office (CSO) to sign an Alarm System Description Form for specified conditions before a CRZH certificate will be issued to ensure contractors coordinate with their CSA/CSO prior to installing an alarm system. The local DSS Field Office will sign the form as the CSO for DoD contractor facilities. Conditions requiring CSO approval include: Requests for (1) Alarm Coverage other than Extent 3, (2) Alarm System with Non-Line Security, (3) Monitoring utilizing Data Networks via the Internet, or Internet Protocol (IP) Addresses, (4) Law Enforcement as the Remote Monitoring Station, (5) Law Enforcement as the Investigator, (5) Contractor Representative (non-professional guard) as the Investigator, and (6) Investigator Response Times other than 15 minutes. A CRZH Certificate will be invalid if the CSO has not signed the System Description Form authorizing an exception.

15. Q&As.

Q: How can I receive a copy of the Underwriters Laboratories (UL) Inc., Standard For Safety, National Industrial Security Systems, UL 2050 and/or the Alarm System Description Form?

A: Requests for the UL 2050, and/or the Alarm System Description Form should be made directly to one of the following UL Regional Offices.

West

Underwriters Laboratories, Inc.
1655 Scott Boulevard
Santa Clara, CA 95050-4169
(408) 985-2400

Mid-West

Underwriters Laboratories, Inc.
333 Pfingsten Road
Northbrook, IL 60062-2096
(847) 272-8800

Northeast

Underwriters Laboratories, Inc.
1285 Walt Whitman Road
Melville, NY 11747-3081
(631) 271-6200

Southeast

Underwriters Laboratories, Inc.
12 Laboratory Drive
Research Triangle Park
North Carolina, 27709-3995
(919) 549-1400

Q: I have grandfathered guards as supplemental controls for existing Closed Areas and containers. If I establish a new Closed Area, can I continue to utilize my grandfathered guards or must I alarm the new Closed Area?

A: Provided there were no breaks in the utilization of the guards; there are no specific contractual requirements for alarms and the Closed Area does not require open storage, you may utilize the grandfathered guards as supplemental controls for the new Closed Area.

Attachment

PROVIDED BY UK GOVERNMENT

RESTRICTED SECURITY CONDITIONS OVERSEAS

Definitions

1. The term "Authority" means Contracting Authority.

Security grading

2. The Authority shall issue a RESTRICTED Aspects Letter which shall define the RESTRICTED matter that is furnished, or which is to be developed, under this Contract. The Contractor shall mark all RESTRICTED documents which he originates or copies during the Contract in accordance with the RESTRICTED Security Aspects Letter.

Protection of RESTRICTED information

3. Except with the consent in writing of the Authority, the Contractor shall not disclose the Contract or any provision thereof to any person other than a person employed by the Contractor. It must be confined to those members of the staff whose access to the information is essential for the purpose of his duties.

4. Except with the consent in writing of the Authority the Contractor shall not make use of the Contract or any information issued or furnished by or on behalf of the Authority otherwise than for the purpose of the Contract, and, save as provided for in Clause 5 the Contractor shall not make any article or part thereof similar to the Articles for any other purpose.

5. Subject to any rights of Third Parties, nothing in this Condition shall, however, constrain the use for any purpose by the Contractor of any specifications, plans, drawings and other documents, the rights of which vest in him otherwise than as a result of work carried out under this Contract.

6. Any samples or patterns or any specifications, plans, drawings or any other documents issued by or on behalf of the Authority for the purposes of the Contract remain the property of the Authority and must be returned on completion of the Contract.

7. When not in use RESTRICTED documents must be stored under lock and key.

Loss

8. Any loss of a RESTRICTED document should be reported without delay to the Authority.

Transmission

9. RESTRICTED documents should be transmitted in such a way as to ensure that no unauthorised person has access. Postal transmissions outside of the company must be in at least one envelope/package. Commercial Couriers may be used, however, transmission via public networks such as the Internet or any other form of electronic connectivity is not permitted without the use of encryption mutually acceptable to the appropriate security authorities.

Use of IT Systems

10. The following Accreditation requirements describe the minimum security requirements for processing and accessing Restricted information on IT systems.

(1) Control of physical access to all hardware elements of the IT system.

(2) Identification and Authentication (ID&A) All systems should have the following functionality:

(a) Up-to-date lists of authorised users

(b) Positive identification of all users at the start of each processing session

(c) An agreed means of transmitting the Restricted data (see paragraph 9 above).

(3) Passwords are part of most ID&A, Security Measures. Passwords should be 9 characters long and should include numeric and "special" characters (if permitted by the system) as well as alphabetic characters.

(4) Internal Access Control - All systems should have internal Access Controls to prevent unauthorised users from accessing or modifying the data.

"This document cannot describe the detailed functions that must be provided for this purpose. As a general rule, any communication path between an unauthorised user and the data can be used to carry an attack or leak data. It is for the implementers to identify possible means of attack and ensure that they are blocked."

(5) Security Accounting and Audit - Security relevant events fall into two categories, namely legitimate events and violations.

(a) The following events should always be recorded:

i. All log on attempts whether successful or failed.

ii. Log off (including time out where applicable).

iii. The creation, deletion or alteration of access rights and privileges.

iv. The creation, deletion or alteration of passwords.

(b) For each of the events listed above, the following information is to be recorded:

i. Type of event,

ii. User ID,

iii. Date & Time

iv. Device ID

The accounting records should have a facility to provide the System Manager with a hard copy of all or selected activity. There should also be a facility for the records to be printed in an easily readable form. All security records are to be inaccessible to users without a need to know.

If the operating system is unable to provide this then the equipment should be protected by physical means when not in use ie locked away or the hard drive removed and locked away.

(6) Integrity & Availability – The following supporting measures should be implemented:

(a) Provide general protection against normally foreseeable accidents/mishaps and known recurrent problems (e.g. viruses and power supply variations)

(b) Defined Business Contingency Plan

(c) Data backup with local storage

(d) Anti Virus Software (Implementation, with updates, of an acceptable industry standard Anti-virus software).

(7) Logon Banners - Wherever possible, a "Logon Banner" should be provided to summarise the requirements for access to a system which may be needed to institute legal action in case of any breach occurring.

A suggested format for the text depending on national legal requirements could be:

"Unauthorised access to this computer system may constitute a criminal offence"

(8) Unattended Terminals - Users are to be automatically logged off the system if their terminals have been inactive for some predetermined period of time, to prevent an attacker making use of an unattended terminal.

(9) Computer systems should not be connected direct to the Internet unless protected by a firewall.

PROVIDED BY UK GOVERNMENT

(10) Before IT storage media (e.g. disks) are disposed an erasure product should be used to overwrite the data. This is a more thorough process than deletion of files which does not remove the data.

Sub-Contracts

11. The Contractor may Sub-contract any elements of this Contract to Sub-contractors within its own country or the United Kingdom. When doing so these security conditions must be incorporated within the Sub-contract document. The prior approval of the Authority must be obtained should the Contractor wish to Sub-contract any elements of the Contract to a contractor in a third country.

Destruction

12. As soon as no longer required RESTRICTED information/material should be destroyed in such a way as to make reconstitution very difficult or impossible, for example, by burning, shredding or tearing into small pieces. Unwanted RESTRICTED information/material which cannot be destroyed in such a way should be returned to the Authority.

Interpretation

13. Advice regarding the interpretation of the above requirements should be sought from the Authority.